

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

FILED
RICHARD W. NAGEL
CLERK OF COURT

IN THE MATTER OF THE SEARCH OF
1936 FAIRFAX AVENUE CINCINNATI,
OHIO 45207 AND THE GOLD MERCEDES
LICENSE PLATE HHZ3434

Case No.

1:18MJ-544

2018 SEP 11 AM 9:40

U.S. DISTRICT COURT
SOUTHERN DIST OHIO
WEST DIV CINCINNATI

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Mary P. Braun, a Detective with the Cincinnati Police Department and a Task Force Officer with the Federal Bureau of Investigation (FBI), being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been employed as a Police Specialist with the Cincinnati Police Department since 2004, and for the past eight years have been assigned to the Regional Electronics Computer Investigations (RECI) Task Force working on crimes involving computers and computer based crimes against children and others. I have become familiar with the methods and schemes employed by persons who trade and collect child pornography as well as the manner in which adults seduce children for hands-on offenses. I have investigated federal criminal violations related to crimes against children, child pornography, and human trafficking. I have received formal training in the investigation of these matters at the Cincinnati Police Academy, the Federal Bureau of Investigation, and the National Center for Missing and Exploited Children, through other in-service training, and through private industry. As part of the Federal Bureau of Investigation's Violent Crimes Against Children/Child Exploitation Task Force, in 2011, I was deputized by the United States Marshals Service as a Special Deputy United States Marshal, thereby authorized to seek and execute arrest and search warrants supporting a federal task force. During my career as a Detective and Task Force Officer, I have participated in various investigations involving computer-related offenses and executed numerous search warrants to include those involving searches and seizures of computers, computer equipment, software, and electronically stored information. I have received both formal and informal training in the

detection and investigation of computer-related offenses. As part of my duties as a Task Force Officer, I investigate criminal violations relating to child exploitation and child pornography including the illegal distribution, transmission, receipt, and possession of child pornography.

2. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

3. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2251(a) (Production of Child Pornography), 18 U.S.C. § 2252/2252A (Possession, Receipt, & Distribution of Child Pornography), and 18 U.S.C. § 2422 (Coercion and Enticement) have been committed by DAVID LAMONT BASKIN (DOB XX/XX/1970). This Affidavit is submitted in support of Applications for search warrants for the following:

a. The residence located at 1936 FAIRFAX AVENUE CINCINNATI, OHIO 45207; as more fully described in Attachment A-1.

b. The vehicle which is a gold Mercedes station wagon with Ohio License Plate HHZ3434; as more fully described in Attachment A-2.

4. The above noted residence and vehicle are more fully described in Attachments A-1 and A-2. The purpose of these Applications is to seize evidence of violations of 18 U.S.C. §§§§ 2251, 2252, 2252A, and 2422. The items to be searched for and seized are described more particularly in Attachments B.

PERTINENT FEDERAL CRIMINAL STATUTES

5. This investigation concerns alleged violations of 18 U.S.C. §§§§ 2251, 2252, 2252A, and 2422 relating to the sexual exploitation of minors.

- a. 18 U.S.C. § 2251(a) prohibits knowingly producing a visual depiction of a minor engaged in sexually explicit conduct, using materials that affect interstate commerce.
- b. 18 U.S.C. § 2252(a)(1) prohibits knowingly transporting or shipping in interstate or foreign commerce, by computer or mail, any visual depiction of minors engaging in sexually explicit conduct.

- c. 18 U.S.C. § 2252(a)(2) prohibits knowingly receiving or distributing, by computer or mail, any visual depiction of minors engaging in sexually explicit conduct that has been mailed, shipped, or transported in interstate or foreign commerce. That section also prohibits knowingly reproducing any visual depiction of minors engaging in sexually explicit conduct for distribution in interstate or foreign commerce by any means, including by computer or the mail.
- d. 18 U.S.C. § 2252(a)(4) prohibits possessing one or more books, magazines, periodicals, films, or other materials which contain visual depictions of minors engaged in sexually explicit conduct that have been transported in interstate or foreign commerce, or that were produced using materials that had traveled in interstate or foreign commerce.
- e. 18 U.S.C. § 2252A(a)(1) prohibits knowingly mailing, transporting, or shipping child pornography in interstate or foreign commerce by any means, including by computer.
- f. 18 U.S.C. § 2252A(a)(2) prohibits knowingly receiving or distributing any child pornography that has been mailed or shipped or transported in interstate or foreign commerce by any means, including by computer.
- g. 18 U.S.C. § 2252A(a)(3)(A) prohibits a person from knowingly reproducing child pornography for distribution through the mail or in interstate or foreign commerce by any means, including by computer.
- h. 18 U.S.C. § 2252A(a)(3)(B) prohibits knowingly advertising, promoting, presenting, distributing, or soliciting through the mail, or using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means any material in a manner that reflects the belief or is intended to cause another to believe that the material is or contains a visual depiction of an actual minor engaging in sexually explicit conduct, or an obscene visual depiction of a minor engaging in sexually explicit conduct.
- i. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing any book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, shipped, or

transported in interstate or foreign commerce by any means, including by computer.

- j. 18 U.S.C. § 2422 states in part that whoever knowingly persuades, induces, entices, or coerces any individual to travel in interstate or foreign commerce, or in any Territory or Possession of the United States, to engage in prostitution, or in any sexual activity for which any person can be charged with a criminal offense, or attempts to do so. Additionally, it provides that whoever, using the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States knowingly persuades, induces, entices, or coerces any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempts to do so. Additionally, it is a crime in the state of Ohio for a person over the age of 18 to engage in sexual conduct with another, who is not the spouse of the offender, when the offender knows the other person is thirteen years of age or older but less than sixteen years of age, or the offender is reckless in that regard. Ohio Rev. Code Ann. § 2907.04 (Unlawful Sexual Conduct With A Minor).

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachments to this Affidavit:
 - a. **“Child Pornography”** includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).
 - b. **“Visual depictions”** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).
 - c. **“Minor”** means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).

- d. **“Sexually explicit conduct”** means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person (see 18 U.S.C. § 2256(2)).
- e. **“Internet Service Providers”** or **“ISPs”** are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.
- f. An **Internet Protocol address**, also referred to as an **IP address**, is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as “octets,” ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).

- g. A network **“server,”** also referred to as a **“host,”** is a computer system that has been designated to run a specific server application or applications and provide requested services to a **“client”** computer. A server can be configured to provide a wide variety of services over a network, including functioning as a web server, mail server, database server, backup server, print server, FTP (File Transfer Protocol) server, DNS (Domain Name System) server, to name just a few.
- h. A **client** is the counterpart of a server or host. A client is a computer system that accesses a remote service on another computer by some kind of network. Web browsers (like Internet Explorer or Safari) are clients that connect to web servers and retrieve web pages for display. E-mail clients (like Microsoft Outlook or Eudora) retrieve their e-mail from their Internet service provider's mail storage servers.
- i. **“Domain Name”** refers to the common, easy to remember names associated with an Internet Protocol address. For example, a domain name of **“www.usdoj.gov”** refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first level, or top level domains are typically **“.com”** for commercial organizations, **“.gov”** for the governmental organizations, **“.org”** for organizations, and, **“.edu”** for educational organizations. Second level names will further identify the organization, for example **“usdoj.gov”** further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, **www.usdoj.gov** identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government. The Domain Name System, also referred to as DNS, is a system of servers connected to each other using a common system of databases that resolve a particular domain name, such as **“www.usdoj.gov,”** to its currently assigned IP address (*i.e.*, 149.101.1.32), to enable the follow of traffic across the Internet.
- j. **“Log Files”** are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by

remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

- k. **“Hyperlink”** (often referred to simply as a “link”) refers to a navigation element in a web page or document that automatically brings the referred information (a.k.a. “resource”) to the user when the navigation element is selected by the user. Hyperlinks are part of the foundation of the World Wide Web, but are not limited to a website for HTML.
- l. **“Website”** consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).
- m. **“Uniform Resource Locator”** or **“Universal Resource Locator”** or **“URL”** is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website’s home page file in the Web browser’s address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.
- n. The terms **“records,” “documents,”** and **“materials,”** as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

CHARACTERISTICS OF COLLECTORS OF CHILD PORNOGRAPHY

7. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereafter “collectors”):

- a. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.
- b. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often have companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature and sexual aids.
- c. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce, convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.
- d. Collectors almost always possess and maintain their “hard copies” of child pornographic images and reference materials (*e.g.*, mailing and address lists) in a private and secure location. With the growth of the Internet and computers, a large percentage of most collections today are in digital format. Typically these materials are kept at the collector’s residence for easy access and viewing. Collectors usually place high value on their materials because of the difficulty, and legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods of time, even for years. Collectors often

discard child pornography images only while “culling” their collections to improve their overall quality.

- e. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography distributors/collectors, including contact information like email addresses, and may conceal such correspondence as they do their sexually explicit material.
- f. Collectors prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.
- g. Subscribers to websites that are primarily designed to provide child pornography have a strong likelihood of being collectors of child pornography. This high degree of correlation between subscription and collection behavior has been repeatedly confirmed during several recent nationwide law enforcement initiatives, including ICE’s “Operation Emissary” and the FBI’s “Ranchi message board” investigation. For example, in the “Ranchi” investigation a national take-down occurred during the week of March 1, 2007. Approximately 83 subjects were contacted, 28 by court-authorized search warrants and 55 by “knock and talks.” Of the 83 contacts, 46 individuals (or 55%) confessed to accessing the Ranchi message board and/or downloading child pornography from Ranchi. Multiple other new cases were opened without confessions based on strong evidence obtained during the Ranchi search warrants and knock-and-talks.

USE OF COMPUTERS AND THE INTERNET WITH CHILD PORNOGRAPHY

8. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other, as well the methods that individuals will use to interact with and sexually exploit children. Computers serve four functions in connection with child pornography: production; communication; distribution and storage.

- h. **Production:** Pornographers can now produce both still and moving images directly from a common video camera. The camera is attached, using a cable, directly to the computer using a device called a video capture board. This device turns the video output into a form that is usable by computer programs. The output of the video

camera can be stored, manipulated, transferred or printed directly from the computer. The captured image can be edited (*i.e.*, lightened, darkened, cropped, digitally enhanced, *etc.*) with a variety of commonly available graphics programs. The producers of child pornography can also use scanners to convert hard-copy photographs into digital images.

- i. **Communication.** Previously, child pornography collectors had to rely on personal contact, U.S. mail, and telephonic communications in order to sell, trade, or market pornography. Today most communications associated with the trafficking of child pornography occur via the obscurity and relative anonymity of the Internet. A device known as a modem allows any computer to connect to the Internet via telephone lines or broadband Internet connections. Once connected to the Internet, individuals search for and/or offer to distribute child pornography in a wide variety of ways. Many individuals congregate in topic-based Internet chat rooms implicitly or explicitly dedicated to child pornography. Online discussions in these chat rooms are usually done via instant message (or "IM"), and individuals may then establish one-on-one chat sessions involving private messages (or "PMs"), visible only to the two parties, to trade child pornography. These child pornography images may be sent as attachments to the PMs, or they may be sent separately via electronic mail between the two parties. Pedophile websites communicate advertisements for the sale of child pornography, and individuals may order child pornography from these websites using email or send order information from their web browser (using HTTP computer language). Some individuals communicate via Internet Relay Chat (IRC) to discuss and trade child pornography images. It is not uncommon for child pornography collectors to engage in mutual validation of their interest in such material through Internet-based communications.
- j. **Distribution.** Computers and the Internet are the preferred method to distribute child pornography. As discussed above, such images may be distributed via electronic mail (either as an attachment or embedded image), or through instant messages as attachments. Child pornography is regularly downloaded from servers or Usenet newsgroups via a method known as FTP (file transfer protocol). Child pornography images are also distributed from websites via client computers web browsers downloading such images via HTTP (Hyper Text Transfer Protocol). Peer-to-peer

networks such as LimeWire and Gnutella are an increasingly popular method by which child pornography images are distributed over the Internet.

- k. **Storage.** The computer's capability to store images in digital form makes it an ideal repository for pornography. A single floppy disk can store dozens of images and hundreds of pages of text. The size of computer hard drives used in home computers has grown tremendously within the last several years. Hard drives with the capacity of two hundred (200) gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Remote storage of these images on servers physically removed from a collector's home computer adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

BACKGROUND REGARDING SEIZURE OF COMPUTERS

9. As stated, the investigation has determined that one or more computers are have been used as an instrumentality in the course of, and in furtherance of, the offenses described above. Moreover, it is reasonable to believe that records and evidence are being stored in electronic form. This includes computer hard-drives, disks, CDs and other similar electronic storage devices.

10. As indicated above, computer hardware is used to save copies of files and communications, while printers are used to make paper copies of same. Programs loaded on the drives are the means by which the computer can send, print and save those files and communications. Finally, password and security devices are often used to restrict access to or hide computer software, documentation or data. Each of these parts of the computer is thus integrated into the entire operation of a computer. In order to best evaluate the evidence, the computers—and all of the related computer equipment described above—should be available to a computer investigator/analyst.

Forensic Imaging

11. An important step that is ordinarily part of an expert's forensic examination of a computer involves attempting to create an electronic "image" of those parts of the computer that are likely to store the evidence, fruits, instrumentalities, or contraband relating to the applicable offense. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files.

12. Special software, methodology and equipment are used to obtain forensic images. Among other things, forensic images normally are "hashed," that is, subjected to a mathematical algorithm to the granularity of 10^{38} power, which is an incredibly large number that is much more accurate than the best DNA testing available today. The resulting number, known as a "hash value" confirms that the forensic image is an exact copy of the original and also serves to protect the integrity of the image in perpetuity. Any change, no matter how small, to the forensic image will affect the hash value so that the image can no longer be verified as a true copy.

Forensic Analysis

13. After obtaining a forensic image, the data will be analyzed. Analysis of the data following the creation of the forensic image is a highly technical process that requires specific expertise, equipment and software. There are literally thousands of different hardware items and software programs that can be commercially purchased, installed and custom-configured on a user's computer system. Computers are easily customized by their users. Even apparently identical computers in an office environment can be significantly different with respect to configuration, including permissions and access rights, passwords, data storage and security. It is not unusual for a computer forensic examiner to have to obtain specialized hardware or software, and train with it, in order to view and analyze imaged data.

14. Analyzing the contents of a computer, in addition to requiring special technical skills, equipment and software also can be very tedious. It can take days to properly search a single hard drive for specific data. Searching by keywords, for example, often yields many thousands of "hits," each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. The computer may have stored information about the data at issue: who created it; when it was created; when it was last accessed; when it was last modified; when was it

last printed; and when it was deleted. Operation of the computer by non-forensic technicians effectively destroys this and other trace evidence.

15. Moreover, certain file formats do not lend themselves to keyword searches. Keywords search for information in text format. Many common electronic mail, database and spreadsheet applications do not store data as searchable text. The contents of Adobe “.pdf” files are not searchable via keyword searches. The data is saved in a proprietary non-text format. Microsoft Outlook data is an example of a commonly used email program that stores data in a non-textual, proprietary manner—ordinary keyword searches will not reach this data. Documents printed by the computer, even if the document never was saved to the hard drive, are recoverable by forensic examiners, yet they are not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. Similarly, faxes sent to the computer are stored as graphic images and not as text.

16. Analyzing data on-site has become increasingly impossible as the volume of data stored on a typical computer system has become mind-boggling. For example, a single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Computer hard drives are now capable of storing more than 100 gigabytes of data and are commonplace in new desktop computers. And, this data may be stored in a variety of formats or encrypted. The sheer volume of data also has extended the time that it takes to analyze data in a laboratory. Running keyword searches takes longer and results in more hits that must be individually examined for relevance. Even perusing file structures can be laborious if the user is well-organized. Producing only a directory listing of a home computer can result in thousands of pages of printed material most of which likely will be of limited probative value.

17. Based on the foregoing, searching any computer or forensic image for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques, and may take weeks or even months. Keywords need to be modified continuously based upon the results obtained. Evidence in graphic file format must be laboriously reviewed by examiners. Criminals can mislabel and hide files and directories, use codes to avoid using keywords, encrypt files, deliberately misspell certain words, delete files, and take other steps to defeat law enforcement.

Persistence of Digital Evidence

18. Computers store data, both on removable media (for example, CDs and floppy diskettes) and internal media, in ways that are not completely known or controlled by most users. Once stored, data is usually not destroyed until it is overwritten. For example, data that is "deleted" by a user is usually not actually deleted until it is overwritten by machine processes (rather than user decision) that decide where to store data and when overwriting will occur. Therefore, files and fragments of files and other data may easily last months, if not years, if the storage media is retained.

19. Typically, computer forensics focuses on at least three categories of data. These are: 1) **active data** – such as current files on the computer, still visible in file directories and available to the software applications loaded on the computer; 2) **latent data** – such as deleted files and other data that resides on a computer's hard drive and other electronic media in areas available for data storage, but which are usually inaccessible without the use of specialized forensic tools and techniques; and 3) archival data – such as data which has been transferred or backed up to other media such as CDs, floppy disks, tapes, and ZIP disks.

20. **Active data** includes not only files created by and with the user's knowledge, but also may include items such as Internet history log files, system registry files (listing all the systems and software applications installed on a computer, including the dates of installation, use, and deletion), and date/time file stamps automatically created that identify when files were created, modified, and last accessed.

21. **Latent data** includes data retained and stored on computer media in "unallocated" and "slack" space. Unallocated space refers to space on a hard drive that is available for the storage of new data. Slack space refers to any leftover space that remains when an active file is stored in particular location on the hard drive that is akin to an empty shelf in a closet containing other full shelves. Deleted files and other latent data that has not been overwritten by new data or files often may be accessed by a qualified forensic examiner from the unallocated and slack space on a computer user's hard drive months and years after such data was created by the user or the computer's operating system.

22. I know, based upon my training and experience, that a qualified forensic examiner may use knowledge of the mechanisms used to store electronic data to unlock and to uncover the activities of a computer's user years after the fact by examination of active, latent, and archival

data. Through the use of proper computer forensic techniques such data and evidence of criminal offenses may be recovered, notwithstanding the passage of time since a crime occurred.

Conclusion Regarding Forensic Analysis Procedures

23. In light of these difficulties, I request permission for investigators to remove to a forensically-secure location the computers and computer-related equipment as instrumentality(ies) of the crimes, and to use whatever data analysis techniques reasonably appear necessary to locate and retrieve digital evidence within the scope of this warrant. Such action will greatly diminish the intrusion of law enforcement into the premises and will ensure that evidence can be searched for without the risk of losing, destroying or missing the information/data for which there has been authorization to search.

24. Therefore, it is respectfully requested that the warrant sought by this application authorize the search and seizure for all "computer hardware," "computer software" and documents, which are more fully set-out and explained above, and further authorize a full physical and forensic examination of the seized items at a secure location.

PROBABLE CAUSE

25. In March, 2018, your affiant was contacted by Hamilton County Jobs and Family Services Caseworker Jennifer Byers regarding Minor Victim (date of birth XX/XX/04), at the time a 13 year old female in her custody, who was six months pregnant. Minor Victim had been placed in foster care and was residing in Greenville, Ohio. Minor Victim told Byers that she had had met a man on a telephone chat line. She stated that his name was David Baskin and she thought he was 30 years old. They began a sexual relationship, meeting often in hotels in the Cincinnati, Ohio area.

26. Minor Victim had been attending middle school, where she was caught sending naked images of herself to older men. Your affiant contacted Officer Jeremy Hyden of the Arcanum Police Department where he was assigned as the School Resource Officer at Minor Victim's school. Officer Hyden stated that the school's principal, had been contacted by Minor Victim's foster mother. The foster mother had been looking through Minor Victim's school issued computer and found pornographic images that were shared on Facebook Messenger. The

foster mother and Minor Victim met with Officer Hyden. They both signed a Consent to Search for Minor Victim's Facebook Messenger account.

27. Officer Hyden saw a chat between Minor Victim and David Lamont Baskin that contained sexually explicit language and child pornography. He took several screenshots of the conversation:

a. On November 11, 2017:

- Baskin: "Have you been playing with that pussy"
- Minor Victim: "yeah"
- Baskin: "Can you play with that pussy now for me"
- Minor Victim: "I just did this morning"
- Baskin: "Can we do it again now"
- Minor Victim: "no bc my foster mom is up" "but later"

b. Also on November 11, 2017:

- Baskin: "Daddy wanna see that pussy go in the bathroom and take some pictures"
- Minor Victim: "later wen she leaves"
- Baskin then sends a video of a woman performing oral sex on an adult male.

c. On November 12, 2017, Minor Victim sent Baskin an image of her naked breasts, and then began a conversation about their ages:

- Minor Victim: "whats ur birth year again is it 1987"
- Baskin: "Yeah how you know"
- Minor Victim: "subtraction $2017 - 30 = 1987$ " "whats my full birth year bc ik urs"
- Baskin: "idk"
- Minor Victim: "its april 10 2004" "urs july 9 1987"
- Baskin: "ok I'll remember"

d. On November 15, 2017, Minor Victim sent Baskin another image of her naked breasts.

- Baskin: "Omg nice" "Pussy picture"
- Minor Victim: "later I can't take it now later"

e. On November 16, 2017, Baskin sent a picture of his face to Minor Victim.

- f. Minor Victim sent Baskin another image of her naked breasts and a close up image of her vagina on November 21, 2017.
- g. Baskin sent her two more images of his face on November 23, 2017.

28. Your affiant searched OHLEG and RCIC for David Baskin and found David Lamont Baskin, Cincinnati, Ohio, date of birth 07/09/1970, Social Security Number XXX-XX-7699. The images that were sent in the Facebook Messenger chats appeared to be the same David Lamont Baskin.

29. On May 3, 2018, Minor Victim was forensically interviewed at Cincinnati Children's Hospital Mayerson Child Advocacy Center. During the interview, Minor Victim stated that she met Baskin on "Live", a telephone chat line. Baskin called her based on the introduction she recorded about herself. He gave her his telephone number, 513-835-9495, and they began calling each other. He would often leave her voicemails with "sexual things".

30. They met in person for the first time in June, 2017. Baskin took her to the Travel Inn in Sharonville, Ohio. Minor Victim stated that Baskin "put his penis in my vagina and mouth...he also touched my vagina with his hand". They regularly met, the last time being in October, 2017.

31. Minor Victim stated that they exchanged naked images of each other and that it was Baskin's idea. She also said that he told her "don't tell anybody about me because I don't want to go to jail".

32. Minor Victim was shown an image of David Lamont Baskin. She identified him as the David Baskin that she met and had sexual intercourse with.

33. Based on the screenshots that were recorded by Officer Hyden, and the statements made by Minor Victim, on July 31, 2018 a federal search warrant for Baskin and Minor Victim's Facebook accounts was signed by Judge Stephanie K. Bowman, of the Southern District of Ohio. On or about August 6, 2018, your affiant received over 7500 pages of results for Baskin and 1400 pages for Minor Victim.

34. According to Minor Victim's Facebook account records, Baskin sent her a friend request on October 19, 2017, which she accepted.

35. In addition to the screenshots that were captured by Officer Hyden and referenced earlier, the following chats between Minor Victim and Baskin were recovered.

a. On November 11, 2017:

- Minor Victim: "can I get a pic of u"
- Baskin: "Okay baby"
- Baskin sends an image of him sitting on the porch of 1936 Fairfax
- Baskin: "Send daddy a picture"
- Minor Victim sends him an image of her face
- Baskin: "Cute send daddy a pussy picture"
- Minor Victim: "cant but later"

b. A little later on November 11, 2017:

- Baskin: "lookin at them titties....on that picture you sent me"
- Baskin: "it look like they getting big"
- Minor Victim: "ikr" (I know right)
- Baskin: "Have you gained any weight"
- Minor Victim: "idk...Im 120"

36. On November 12, 2017:

- Baskin: "When I do see you again daddy gonna fuck yo brains out"
- Baskin: "Mouth pussy and ass"

37. On November 13, 2017, Minor Victim sent Baskin an image of her naked breasts.

38. On November 16, 2017, Minor Victim sent Baskin another image of her naked breasts.

- Baskin: "Omg nice....Pussy picture"

39. On November 21, 2017, Minor Victim sent Baskin another image of her naked breasts and then a close up image of her vaginal area.

40. On November 26, 2017:

- Minor Victim: "so what u wanna talk about"
- Baskin: "Suck and fuckin"
- Minor Victim: "Ok start"
- Baskin: "I wanna lick on you neck and kiss you"

41. One of the telephone numbers that Facebook had listed as a "Cell Verified" number was 513-835-9495, the same number that Baskin used to communicate with Minor Victim.

42. On October 17, 2017 Baskin's Facebook page showed that he became friends with Minor Victim. Over the next few days, Baskin searched for her several times, using different spelling variations of her name.

43. During several postings, Baskin states that he is having a party at his house and lists the address as 1936 Fairfax Avenue, Cincinnati, Ohio 45207. He also posted several images of him sitting on the porch of 1936 Fairfax Avenue. Additionally, he has images of himself in front of the detached garage, both with the door closed and with him standing in the open doorway.

44. On 1/20/18, Baskin posted an image of a gold Mercedes station wagon, indicating it was his with the caption, "My new Bitch! Elvirah".

45. On or about 8/15/18, your affiant observed the area of 1936 Fairfax Avenue, Cincinnati, Ohio 45207. There was a gold Mercedes station wagon parked directly in front of 1936 Fairfax Avenue, with Ohio License Plate HHZ3434, which is registered to Amy Hamilton, date of birth XX/XX/1976, Social Security Number XXX-XX-1332. Her address is listed as 1936 Fairfax Avenue, Cincinnati, Ohio 45207. According to the Hamilton County Auditor's website, Hamilton is listed as the owner of that home.

46. Hamilton and Baskin are in numerous images together that are posted to Facebook. It appears they are in a relationship. In several conversations they discuss living together.

a. On November 12, 2017:

- Hamilton: "They look like they are dancing in our kitchen."

b. On December 16, 2017:

- Hamilton: "Love u"
- Baskin: "Love you more"

c. On June 12, 2018:

- Hamilton: "I'm coming home for lunch. Are you at home?"
- Baskin: "Yes"
- Hamilton: "Ok. We'll try to find it when I get home"

47. On July 24, 2018, Facebook listed the Last Location of a Mobile Device associated with the account as Latitude 39.135.2925, Longitude -84.466555. The accuracy of those coordinates was 15 meters. When those coordinates are put in a GPS coordinate converter, the address is 1934 Fairfax Avenue, Cincinnati, Ohio 45207. This house is next door to 1936 Fairfax and is within the 15 meters of accuracy

48. On or about August 21, 2018 at approximately 1:00 PM, your affiant went to the SUBJECT PREMISES and observed the house. The house has the number 1936 next to the front door. Additionally, there is detached garage directly behind the house that is accessible through an alley.

CONCLUSION

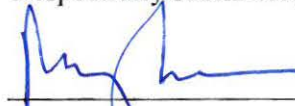
49. Based on the forgoing, I request that the Court issue the proposed search warrants.

REQUEST FOR SEALING

50. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all

of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,



Mary P. Braun
Task Force Officer
Federal Bureau of Investigation

Subscribed and sworn to before me on September 11, 2018



STEPHANIE K. BOWMAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-2
Property to Be Searched

A Mercedes-Benz E500 station wagon bearing Ohio License Plate HHZ3434 and Vehicle Identification Number (VIN) WDBUH83JX4X165028, gold in color currently registered to Amy Hamilton at 1936 Fairfax Avenue, Cincinnati, Ohio 45207. See photograph:



ATTACHMENT B

Particular Things to be Seized

The terms "child pornography" and "visual depictions," as used herein, have the same definitions listed in Section III of the attached affidavit, and those definitions are incorporated herein by reference.

1. Computer(s), computer hardware (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives, diskettes, and other memory storage devices), computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.
2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs, including, but not limited to, P2P software.
3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography, or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct.
4. In any format or medium, all child pornography or child erotica.
5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of the computer, or by other means for the purpose of distributing or receiving child pornography, or visual depictions.

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by U.S. mail or by computer, any child pornography or any visual depictions.
7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography or visual depictions.
8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography, or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.
9. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.
10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.
11. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

12. Any and all files, documents, records, or correspondence, in any format or medium (including, but not limited to, network, system, security, and user logs, databases, software registrations, data and meta data), that concern user attribution information.
13. Any and all cameras, film, videotapes or other photographic equipment.
14. Any and all visual depictions of minors in order to compare the images to known and identified minor victims of sexual exploitation.
15. Any and all address books, mailing lists, supplier lists, mailing address labels, and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography or any visual depictions.
16. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to occupancy or ownership of the premises described above, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.
17. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct.
18. Any evidence of the presence or use of a peer-to-peer file sharing program.
19. Any communications, in any format, with Minor Victim.
20. Any images of Minor Victim.
21. Any cellular phone or telephone associated with call number 513-835-9495.
22. Any records, bills, or other documents associated with phone number 513-835-9495.
23. Any receipts, documentation, or information concerning hotel/motels.